Elementos de Criptografia

LMAC, LEIC, MEIC

Exame I - 16 valores

Duração: 3 horas

Grupo I 1.5+2+1.5

1. Considere o sistema criptográfico de transposição $\mathcal{T} = \langle Z_n, Z_n, Z_n, e, d\rangle$ com n par e considere que $P(C = c) = 4/(3n)$ se $c < n/2$ e $P(C = c) = 2/(3n)$ se $c \geq n/2$. Diga, justificando, se $\mathcal{T}$ é incondicionalmente segura. Mostre que existe um sistema criptográfico estocástico $\mathcal{T}'$ tal que $\mathcal{T} \circ \mathcal{T}'$ é incondicionalmente segura.

2. Mostre como é que o fluxo por blocos da cifra de Hill pode ser representado como um fluxo de chaves da cifra de transposição. Mostre que qualquer fluxo por blocos de um sistema criptográfico em que o conjunto de símbolos de mensagem X e de criptogramas Y é Z_n^k pode ser representado por um fluxo de chaves da cifra de transposição sobre Z_n.

3. Descreva sucintamente o algoritmo de cifração do DES e como este pode ser utilizado em blocos.

Grupo II 2.5+3.5

1. Apresente a correcção do esquema de assinatura de RSA. Mostre como pode atacar este sistema se conhecer três das quatro raízes quadradas de um qualquer resíduo quadrático em Z_n.

2. Considere o sistema criptográfico de ElGamal sobre Z_p com gerador α. Considere a seguinte linguagem $L \subseteq Z_{p-1} \times RQ(p)$ tal que $L(x, y) = 1$ sse $x < \log_\alpha y$ e onde $RQ(p)$ é o conjunto dos resíduos quadráticos módulo p. Mostre que se $L \in \mathbf{P}$ então é possível analisar em tempo polinomial o sistema criptográfico de ElGamal, dando um limite superior para a complexidade do seu algoritmo.

Grupo III 2.0+3.0

1. Descreva o esquema de partilha de chaves de Blum, justifique a sua utilização, e mostre a sua correcção.

2. Apresente o sistema de prova de conhecimento nulo baseado no isomorfismo de grafos e demonstre que este está correcto, adequado e que é de conhecimento nulo. Suponha que a Alice deseja que o Bruno se comprometa com um bit b numa certa data t. Esse bit deverá ser conhecido apenas pelo Bruno até que um certo evento aconteça na data $t + k$. Nesta altura o Bruno deverá demonstrar à Alice que se tinha comprometido com b, devendo ser impossível (em tempo polinomial) a Bruno conseguir demonstrar que se tinha comprometido com $1 - b$. Apresente um protocolo para resolver este problema.